Malawer 4

.text: 00401010 push eax

.text: 00401014 push ebx

.text: 00401018 push ecx

.text: 0040101C push WH_Mouse ;hook to Mouse

text: 0040101F call SetWindowsHook()

.text: 00401040 XOR ECX,ECX

.text: 00401044 mov ecx, [EDI] EDI = «path to startup_folder_system»

.text: 00401048 mov edx, [ESI] ESI = path_to_Malware

.text: 0040104C push ecx ;destination folder

.text: 0040104F push edx ; file to be copied

.text: 00401054 call CopyFile();

ANALISI

Crea una funzione che registra il mouse (hook to mouse, arpione al mouse).

Per la persistenza si va a posizionare nel system startup folder e va a copiare i file.

1. Evidenziazione delle chiamate di funzione principali e le relative descrizioni:
    - **SetWindowsHook()**: Questa funzione imposta un hook di Windows per catturare gli eventi del mouse. Il parametro **WH_Mouse** specifica il tipo di hook, che in questo caso sembra essere un hook per gli eventi del mouse.
    - **CopyFile()**: Questa funzione copia un file dal percorso di origine al percorso di destinazione specificato. Nel codice fornito, il percorso di origine è memorizzato nel registro **esi** e il percorso di destinazione è memorizzato nel registro **ecx**.
2. Analisi a basso livello delle singole istruzioni:
    - **.text: 00401010 push eax**: Questa istruzione mette il valore del registro **eax** nello stack, salvando temporaneamente il valore.
    - **.text: 00401014 push ebx**: Questa istruzione mette il valore del registro **ebx** nello stack, salvando temporaneamente il valore.
    - **.text: 00401018 push ecx**: Questa istruzione mette il valore del registro **ecx** nello stack, salvando temporaneamente il valore.
    - **.text: 0040101C push WH_Mouse**: Questa istruzione mette il valore **WH_Mouse** nello stack. **WH_Mouse** sembra essere un valore costante o una variabile associata a un hook di Windows per gli eventi del mouse.

- **.text: 0040101F call SetWindowsHook()**: Questa istruzione chiama la funzione **SetWindowsHook()**.
- **.text: 00401040 XOR ECX, ECX**: Questa istruzione esegue un'operazione di XOR tra il registro **ecx** e se stesso, impostandolo a zero.
- **.text: 00401044 mov ecx, [EDI]**: Questa istruzione sposta il valore della memoria all'indirizzo contenuto nel registro **edi** nel registro **ecx**.
- **.text: 00401048 mov edx, [ESI]**: Questa istruzione sposta il valore della memoria all'indirizzo contenuto nel registro **esi** nel registro **edx**.
- **.text: 0040104C push ecx**: Questa istruzione mette il valore del registro **ecx** nello stack.
- **.text: 0040104F push edx**: Questa istruzione mette il valore del registro **edx** nello stack.
- **.text: 00401054 call CopyFile()**: Questa istruzione chiama la funzione **CopyFile()**.